REMARKS

The Examiner has objected to the specification. Such objections are deemed to be avoided by virtue of the clarifications made hereinabove to the specification.

The Examiner has further objected to the drawings. Such objections are deemed to be avoided by virtue of the clarifications made hereinabove to the drawings.

The Examiner has further rejected Claims 10 and 23 under 35 U.S.C. 112, since "D" is allegedly not defined by the claims. Such rejection is deemed to be avoided by virtue of the clarifications made hereinabove to such claims.

The Examiner has further provisionally rejected Claims 1-25 under 35 U.S.C. 101 as claiming the same invention as that of Claims 1-25 of copending Application No.: 09/836,214. Applicant respectfully disagrees with this rejection. It appears that the Examiner is in error, since copending Application No.: 09/836,214 includes 39 claims, not 25 claims, and further claims significantly different subject matter.

The Examiner has further rejected Claims 1, 3, 11-14, 17, 24, and 25 under 35 U.S.C. 103(a) as being unpatentable over Ioulus: A Framework for Scaleable Secure Multicasing, by Suvo Mittra, hereinafter Mittra, in view of U.S. Patent No. 6,606,706 to Li, hereinafter Li. Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove.

In particular, applicant has amended each of the independent claims to include the subject matter of Claim 4 et al. The Examiner has rejected the subject matter of Claim 4 under 35 U.S.C. 103(a) as being unpatentable over Mittra, in view of Li, and in further view of U.S. Patent No. 6,240,188 to Dondeti, hereinafter Dondeti. Again, applicant respectfully disagrees.

In particular, the Examiner cites the excerpts below from Dondeti to make a prior art showing of applicant's claimed "wherein said subgroup is a self-repairing group, said self-repairing group being operative to update said leaf key independently" (see this or similar language in each of the independent claims).

> "The requirements and desirable characteristics of a secure many-to-many protocol are as follows. A secure group communication scheme must be scalable. More specifically, key distribution overhead must be scalable as the number of members (or senders) in the group increases. All senders must be trusted equally and the group must be operational if at least one sender is operational. It is desirable to distribute access control and dynamic group management tasks to all senders. This allows the joins and leaves to be processed locally, thus avoiding global flooding of control traffic. Distribution of group management tasks also avoids performance bottlenecks and eliminates single points of attack in a multicast group. Finally, the protocol should be able to avoid or detect and eliminate any colluding members or senders efficiently.
>
> The present invention presents a group key management system and method for providing secure many-to-many communication. The system employs a binary distribution tree structure. The binary tree includes a first internal node having a first branch and a second branch depending therefrom. Each of the branches includes a first member assigned to a corresponding leaf node. The first member has a unique binary ID that is associated with the corresponding leaf node to which the first member is assigned. A first secret key of the first member is operable for encrypting data to be sent to other members. The first member is associated with a key association group that is comprised of other members. The other members have blinded keys. A blinded key derived from the first secret key of the first member is transmitted to the key association group. Wherein, the first member uses the blinded keys received from the key association group and the first secret key to calculate an unblinded key of the first internal node. The unblinded key is used for encrypting data that is communicated between members located on branches depending from the first internal node." (col. 2, lines 19-53)

Further, the Examiner argues that Dondeti states that such a modification would make key distribution scaleable to a larger number of users, as it would reduce flooding of control traffic. Whether Dondeti discloses this or not, Dondeti still fails to meet applicant's claims. Namely, the foregoing except, along with the remaining Dondeti reference, fails to even suggest a self-repairing group, let alone a self-repairing group being operative to update a leaf key independently.

To emphasize what is meant by applicant's claimed "self-repairing," now further claimed in each of the independent claims is a requirement that "each of said members of said subgroup is capable of independently updating a shared interior node key" (see this or similar language, but not identical, in each of the independent claims). Thus, applicant now teaches and claims a subgroup wherein each of the members thereof are each independently empowered to update the shared interior key on their own.

Dondeti actually *teaches away* from such technique in that it requires collaboration of a secret key of a first member and a blind key of the other members. Thus, not only is applicant's claimed technique novel, but also *unobvious* in view of the Examiner's proposed combination.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations. Again, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the Examiner's application of the prior art to the dependent claims is further replete with deficiencies. Just by way of example, the Examiner relies on pages 282-283 from Mittra to meet applicant's claimed

"notifying a plurality of members of said group that said at least one member has been evicted" (see Claim 14 et al.). After carefully reviewing such excerpt, however, it is clear that Mittra makes no such disclosure.

Further, the Examiner relies on the following excerpt from Dondeti to meet applicant's claimed "wherein said self-repairing group uses a reusable power set" (see Claim 5 et al.).

> "Members are represented by the leaves of a binary key distribution tree 26. Each member 22 generates a unique secret key 28 for itself and each internal node key is computed as a function of the secret keys of its two children. All secret keys 28 are associated with their blinded versions 30, which are computed using a one-way function 32. Each member 22 holds all the unblinded keys of nodes that are in its path to the root and the blinded keys of nodes that are siblings of the nodes in its path to the root. The contribution of the unique secret key toward the computation of the root key gives each member 22 partial control over the group. A join/leave requires only the keys in the path to the root from the joining/departing host to be changed. Thus, each membership change necessitates only O(log n) messages where n is the number of members in the group. Thus the protocol is scalable." (col. 3, lines 47-63)

However, after carefully reviewing such excerpt, it is clear that Dondeti does not even suggest a "power set," let alone a "reusable power set," as defined by the specification. At least a portion of such definitions have been further incorporated into the claims, by virtue of the newly added claims noted below.

Still yet, applicant brings to the Examiner's attention the following additional dependent claims that have been added, which include the following subject matter presented for consideration:

> "wherein said updating of said shared interior node key is carried out in a single step" (see Claim 26);
>
> "wherein said updating of said shared interior node key is not dependent on key distribution messages from a root node that update further node keys descending from said shared interior node key" (see Claim 27);

"wherein said reusable power set uses a power set of said members in said subgroup as a basis for group key updates" (see Claim 28);

"wherein said reusable power set includes 2^N sets, where N includes the number of said members" (see Claim 29); and

"wherein said reusable power set includes $2^N - 1$ sets, where N includes the number of said members" (see Claim 30).

A notice of allowance or a specific prior art showing of the exact claim limitations, in combination with the remaining claim limitations, is thus respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. If any fees are due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P090/00.176.01).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172
Telephone: (408) 505-5100